

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. (Currently Amended) A process that monitors network traffic through a
2 monitoring device disposed between a data center and a network for thwarting
3 denial of service attacks on the data center, the process comprises:
4 a detection process to determine if the values of a parameter of network
5 traffic exceed normal values for the parameter to indicate an attack on the data
6 center;
7 a characterization process to build a histogram for the parameter to
8 compute significant outliers in a parameter and classify the attack; and
9 a filtering process for filtering of network packets based on the
10 characterization ~~process~~ process, wherein the filtering process comprises:
11 constructing a master correlation bit vector, wherein bits of the
12 master correlation bit vector correspond to parameter correlations;
13 initializing bits of a packet's correlation bit vector as not
14 suspicious;
15 retrieving a parameter from a parameter suspicious correlation bit
16 vector, which comprises a list of suspicious values for the parameter, to
17 construct the packet's correlation bit vector; and
18 using a value of the packet's correlation bit vector to index the
19 master correlation bit vector.
- 1 2. (Previously Presented) The process of claim 1 wherein, in the
2 characterization process, suspicious parameter values are represented by a bit

3 vector with a 1 in every position corresponding to a "bad" value, and a 0 in every
4 position corresponding to a "good" value.

1 3. (Previously Presented) The process of claim 1 wherein the
2 characterization process comprises:
3 a correlation process that correlates suspicious parameters and determines
4 existence of correlations of those parameters that indicate types of attacks.

1 4. (Original) The process of claim 3 wherein the correlation process is
2 used to reduce dropping of legitimate traffic.

1 5. (Currently amended) The process of claim ~~2~~1 wherein filtering is
2 aggregate filtering.

1 6. (Original) The process of claim 1 wherein parameters include at least
2 one of source IP address, destination IP address, source TCP/UDP ports,
3 destination TCP/UDP ports, IP protocol, IP TTL, IP length, hash of payload
4 fragment, IP TOS field, and TCP flags.

1 7. (Currently Amended) A method for thwarting denial of service attacks
2 on a data center, the method comprising:
3 producing a histogram of received network traffic for at least one
4 parameter of network packets; ~~and~~
5 characterizing an attack based on comparison of a historical histogram
6 with the produced histogram data for one or more ~~parameters~~parameters; and
7 filtering out traffic characterized as part of an attack, wherein filtering out
8 the traffic comprises:
9 constructing a master correlation bit vector, wherein bits of the
10 master correlation bit vector correspond to parameter correlations;

11 initializing bits of a packet's correlation bit vector as not
12 suspicious;
13 retrieving a parameter from a parameter suspicious correlation bit
14 vector, which comprises a list of suspicious values for the parameter, to
15 construct the packet's correlation bit vector; and
16 using a value of the packet's correlation bit vector to index the
17 master correlation bit vector.

1 8. (Currently Amended) The method of claim 7 further comprising:
2 filtering network packets sent to the data center based on whether ~~or not a~~
3 value of ~~the attribute~~ an attribute represented in the ~~current-produced~~ histogram is
4 within a normal range of ~~values~~ the values for the attribute, as determined by
5 comparison to the historical histogram.

1 9. (Currently amended) The method of claim 7 wherein the historical
2 histogram is based on time periods ~~that can range from 1 hour to 1 week or~~
3 ~~more of~~ at least one hour.

1 10. (Currently amended) The method of claim 7 wherein the produced
2 histogram is produced during an attack and over time periods of ~~about~~
3 approximately 10-300 sec or so seconds.

1 11. (Previously Presented) The method of claim 7 further comprising:
2 normalizing the produced and the historical histograms for each
3 parameter; and
4 computing their difference to identify significant outliers that are
5 considered indicators of suspicious traffic.

1 12. (Original) The method of claim 11 further comprising:

2 correlating suspicious parameters to reduce blocking of legitimate traffic.

1 13. (Currently Amended) The method of claim 12 wherein the packet's
2 correlation bit vector contains sufficient bits to represent the ~~whole~~-parameter
3 space.

1 14. (Currently amended) The method of claim 11 further comprising:
2 correlating suspicious parameters to determine ~~existence of correlations~~
3 ~~of a correlation of~~ those parameters that can ~~point to indications of attacks.~~ indicate
4 an attack.

1 15. (Currently Amended) The method of ~~claim 11~~ claim 8 wherein filtering
2 the network packets based on attribute further comprises:
3 producing ~~a master~~ the master correlation ~~vector~~ bit vector from a stream
4 of sampled packets and examining the network packets using a process that is
5 constant-time, independently of the number of correlations or of the number of
6 suspicious values for a parameter.

1 16. (Canceled).

1 17. (Currently amended) The method of ~~claim 16~~ claim 15 wherein
2 filtering the network packets based on attribute further comprises:
3 ~~testing the bit~~ testing bits in the master correlation ~~vector~~ bit vector to
4 decide whether to drop or forward the packet.

1 18. (Currently Amended) The method of ~~claim 7~~ claim 8 wherein ~~attributes~~
2 ~~include~~ the attribute comprises at least one of source IP address, destination IP
3 address, source TCP/UDP ports, destination TCP/UDP ports, IP protocol, IP TTL,
4 IP length, hash of payload fragment, IP TOS field, and TCP flags.

1 19. (Original) The method of claim 7 wherein the method is executed on a
2 data collector.

1 20. (Original) The method of claim 7 wherein the method is executed on a
2 gateway.

1 21. (Currently Amended) A monitoring device for thwarting denial of
2 service attacks on a data center, the monitoring device comprises:
3 a computing device executing:
4 a process to build at least one histogram for at least one parameter of
5 network ~~traffic; and traffic;~~
6 a process to characterize an attack based on a comparison of a historical
7 histogram of the at least one parameter to the built at least one histogram for the
8 at least one ~~parameter; parameter; and~~
9 a process to filter network packets based on characterization, wherein the
10 process to filter the network packets comprises:
11 constructing a master correlation bit vector, wherein bits of the
12 master correlation bit vector correspond to parameter correlations;
13 initializing bits of a packet's correlation bit vector as not
14 suspicious;
15 retrieving a parameter from a parameter suspicious correlation bit
16 vector, which comprises a list of suspicious values for the parameter, to
17 construct the packet's correlation bit vector; and
18 using a value of the packet's correlation bit vector to index the
19 master correlation bit vector.

1 22. (Original) The monitoring device of claim 21 further comprising:

2 a process to correlate suspicious parameters to reduce blocking of
3 legitimate traffic.

1 23. (Original) The monitoring device of claim 21 wherein the
2 characterization process normalizes the historical and built histograms for each
3 parameter and computes their difference to identify significant outliers that are
4 considered indicators of suspicious traffic.

1 24. (Currently Amended) The monitoring device of claim 23 wherein the
2 characterization process produces ~~a master~~the master correlation vector from a
3 stream of sampled packets and examines the sampled packets using a process that
4 is constant-time, independently of the number of correlations or of the number of
5 suspicious values for a parameter.

1 25. (Original) The monitoring device of claim 21 wherein the device is a
2 gateway device that is adaptable to dynamically install filters on nearby routers.

1 26. (Original) The monitoring device of claim 21 wherein the device is a
2 data collector.

1 27. (Original)The monitoring device of claim 21 wherein the parameters
2 include at least one of source IP address, destination IP address, source TCP/UDP
3 ports, destination TCP/UDP ports, IP protocol, IP TTL, IP length, hash of payload
4 fragment, IP TOS field, and TCP flags.

1 28. (Currently Amended) A computer program product residing on a
2 computer readable medium comprising instructions for causing a processor to:
3 build a histogram for a parameter of network ~~traffic; and~~traffic;

4 use the histogram data for the parameter to characterize an ~~attack-attack~~;
5 and
6 filter the network traffic based on characterization of the attack, wherein
7 the instructions to filter the network traffic comprises instructions to:
8 construct a master correlation bit vector, wherein bits of the master
9 correlation bit vector correspond to parameter correlations;
10 initialize bits of a packet's correlation bit vector as not suspicious;
11 retrieve a parameter from a parameter suspicious correlation bit
12 vector, which comprises a list of suspicious values for the parameter, to
13 construct the packet's correlation bit vector; and
14 use a value of the packet's correlation bit vector to index the
15 master correlation bit vector.

1 29. (Canceled).

1 30. (Currently amended) The computer program product of claim 28
2 further comprising instructions to:
3 determine if ~~the values of a parameter exceed~~ a parameter value exceeds a
4 ~~normal values-value~~ for the parameter to indicate an attack on the site.

1 31. (Currently amended) The computer program product of claim 30
2 further comprising instructions to:
3 use the histogram to characterize the attack when it is determined that ~~one~~
4 ~~of the parameters~~ a parameter value exceeds a threshold.

1 32. (Currently Amended) A method of protecting a data center during a
2 denial of service attack, the method comprises:
3 monitoring network traffic through a gateway disposed between the data
4 center and a network:

5 determining if values of at least one parameter exceed normal, threshold
6 values expected for the parameter to indicate an attack on the site;
7 producing a histogram for the at least one parameter of network traffic to
8 characterize the attack by comparing the histogram to at least one historical
9 histogram for that parameter; and
10 filtering out traffic based on characterizing the traffic, which the gateway
11 deems to be part of an ~~attack~~-attack, wherein filtering out the traffic comprises:
12 constructing a master correlation bit vector, wherein bits of the
13 master correlation bit vector correspond to parameter correlations;
14 initializing bits of a packet's correlation bit vector as not
15 suspicious;
16 retrieving a parameter from a parameter suspicious correlation bit
17 vector, which comprises a list of suspicious values for the parameters, to
18 construct the packet's correlation bit vector; and
19 using a value of the packet's correlation bit vector to index the
20 master correlation bit vector.

1 33. (Original) The method of claim 32 further comprising:
2 communicating statistics collected in the gateway to a control center.

1 34. (Original) The method of claim 33 wherein communicating occurs
2 over a dedicated link to the control center via a hardened network.

1 35. (Original) The method of claim 33 wherein the gateway is physically
2 deployed in line in the network.

1 36. (Original) The method of claim 33 wherein filtering occurs on nearby
2 routers.

1 37. (Original) A method to reduce blocking of legitimate traffic in a
2 process to protect a victim site during a denial of service attack, comprises:
3 producing a histogram of network traffic to characterize an attack; and
4 filtering out traffic deemed part of an attack with filtering comprising:
5 constructing a master correlation vector having asserted bits
6 corresponding to the most important parameter correlations;
7 initializing a packet's correlation bit vector to 0, and for every parameter:
8 retrieving the parameter in a parameter suspicious vector to construct the
9 packet' correlation bit vector; and
10 using the value of the packet's correlation bit vector to index into the
11 master correlation bit vector.

1 38. (Original) The method of claim 37 further comprising:
2 testing the indexed bit in the master correlation vector, where if the bit in
3 the master correlation bit vector is a one, the packet is dropped, otherwise the
4 packet is forwarded.

1 39. (Original) The method of claim 37 wherein the master correlation
2 vector is constructed from a stream of sampled packets.

1 40. (Original) The method of claim 37 further comprising:
2 maintaining a correlation bit vector with as many bits as there are
3 parameters; and
4 if a parameter's suspicious vector has a 1 in a bit position corresponding to
5 the parameter's value in a packet, the method further comprises:
6 setting the bit corresponding to the parameter in the packet's correlation
7 vector to 1.